OIPE IAP44
MAY 14 2007
PATENT & TRADEMARK OFFICE

Doc Code: AP.PRE.REQ

PTO/SB/33 (07-05)
Approved for use through xx/xx/200x. OMB 0651-00xx
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Docket Number (Optional)	
SON-2320	

Application Number	Filed
10/041,964-Conf. #4260	January 9, 2002
First Named Inventor: Makoto OKA et al.	
Art Unit: 2134	Examiner: W. S. Powers

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).
Note: No more than five (5) pages may be provided.

I am the

- [ ] applicant /inventor.
- [ ] assignee of record of the entire interest. See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)
- [x] attorney or agent of record. Registration number 24,104 / 40,290
- [ ] attorney or agent acting under 37 CFR 1.34. Registration number if acting under 37 CFR 1.34. _____

Signature

Ronald P. Kananen/Christopher M. Tobin
Typed or printed name

(202) 955-3750
Telephone number

May 14, 2007
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

- [ ] *Total of 1 form is submitted.

OIPE IAP44
MAY 14 2007
PATENT & TRADEMARK OFFICE

Docket No.: SON-2320
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Makoto OKA et al.

Application No.: 10/041,964 | Confirmation No.: 4260

Filed: January 9, 2002 | Art Unit: 2134

For: PUBLIC KEY CERTIFICATE ISSUING SYSTEM, PUBLIC KEY CERTIFICATE ISSUING METHOD, DIGITAL CERTIFICATION APPARATUS, AND PROGRAM STORAGE MEDIUM | Examiner: W. S. Powers

REQUEST FOR PRE-APPEAL BRIEF PANEL REVIEW OF FINAL REJECTION

MS AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

This is in full and timely response to the Final Office Action mailed on April 12, 2007.

The rejections found within the Final Office Action are traversed at least for the following reasons:

Claims 1-36 are present within the above-identified application, with claims 1, 14, 23, and 36 being independent.

Page 4 includes a rejection of claims 1-3, 5, 6, 9, 10, 12-17, 19, 20, 22-25, 27, 28, 31, 32 and 34-36 under 35 U.S.C. § 102(b) in view of U.S. Pat. No. 6,035,402 to Vaeth et al. ("Vaeth").

Vaeth – Vaeth arguably discloses a Virtual Certificate Authority where requests for a certificate and verification information are directed to the Certificate Authority (CA) from a

plurality of entities, *via* a Request Authority (RA). In Vaeth:

- The CA implements generic or specialized certificate functions **based on the requesting entity**. Col. 7, ll. 36-40. Multiple entities may request different certificates via a single RA. The CA issues each type of certificate by using a different crypto-card to perform to associating cryptography functions, thereby creating a **1-to-1 relationship between certificate types and entity types (i.e., 1 certificate per entity)**.

- The absence of a relationship between RAs and types of certificates allows two RAs to obtain similar certificates, and for the implementation of joint certification by multiple RAs . Elements 180 and 188; Col. 7, ll. 49-59.

The Examiner cites Vaeth Col. 7, ll. 41-47, Col. 8, l. 48 – Col 9, l. 12, for the allegation that Vaeth does in fact teach that, "*said identification of the assigned algorithm [is] made with reference to a table that associates the registration authority with the assigned encryption algorithm.*"

The cited portion of Vaeth only indicates that the RA acts as a gatekeeper between the transacting entity and the CA. Col. 8, ll. 35-48. The fact that the RA plays no role in certificate selection allows the RA to process certificates for various types of entities. Col. 8, l. 48 – Col 9, l. 12. There is no indication whatsoever that any information pertaining to the RA plays any role within Vaeth's crypto-card/certification selection scheme. For example, Vaeth selects which algorithms to perform and certifications to issue based on the entity that is requesting the certificate, by associating specific cryptographic functions (or groups of functions) with merchant requests, another with cardholder requests, and yet another with payment gateway requests. Col. 7, ll. 31-32.

Furthermore, the fact that Vaeth's disclosure teaches joint certification and distributed certification further distinguishes Vaeth from a certification selection process based on the requesting RA. If the certificate in Vaeth were assigned based on the requesting RA, then no

two RAs would be able to issue similar certificates and the joint or distributed certification scheme would be impossible. Accordingly, a certification method that selects different certificates based on the requesting RA (as disclosed by applicant) is contrary to purpose of using multiple RAs to issue the same types of certificates (as disclosed by Vaeth).

Thus, Vaeth *fails* to disclose, teach, or suggest that *said identification of the assigned algorithm [is] made with reference to a table that associates the registration authority with the assigned encryption algorithm.*

Withdrawal of this rejection and allowance of the claims is respectfully requested.

Page 11 includes a rejection of claims 4, 7, 26, and 29 under 35 U.S.C. § 103(a) over Vaeth in view of U.S. Pat. No. 6,202,157 to Brownlie et al. ("Brownlie").

Brownlie - Brownlie discloses a network security system capable of applying security policy provisions issued at a centralized authority to various network nodes, which in turn verify the policy provisions using digital signatures associated with the central authority.

However, Brownlie fails to teach or suggest a certification scheme that associates the registration authority with an assigned encryption algorithm.

Thus, Brownlie *fails* to disclose, teach, or suggest that *said identification of the assigned algorithm [is] made with reference to a table that associates the registration authority with the assigned encryption algorithm.*

Withdrawal of this rejection and allowance of the claims is respectfully requested.

Page 12 includes a rejection of claims 8, 18, and 30 under 35 U.S.C. § 103(a) over Vaeth in view of Boneh et al., "On the Importance of Checking Cryptographic Protocols for Faults" ("Boneh").

Boneh - Boneh describes how various authentication protocols can be broken using hardware faults.

However, Brownlie fails to teach or suggest the distribution of encrypted certificates.

Thus, Boneh *fails* to disclose, teach, or suggest that *said identification of the assigned algorithm [is] made with reference to a table that associates the registration authority with the assigned encryption algorithm.*

Withdrawal of this rejection and allowance of the claims is respectfully requested.

Page 12 includes a rejection of claims 11, 21, and 33 under 35 U.S.C. § 103(a) over Vaeth in view of U.S. Patent No. 6,675,296 to Boeyen et al. ("Boeyen")

Boeyen - Boeyen discloses a certificate issuing apparatus and method to facilitate converting certificates between different formats. The Boeyen apparatus employs a series of templates representing different certificate formats, and maps the relevant data between the different formats.

However, Brownlie fails to teach or suggest a certification scheme or associating a registration authority with an encryption algorithm

Boeyen *fails* to disclose, teach, or suggest that *said identification of the assigned algorithm [is] made with reference to a table that associates the registration authority with the assigned encryption algorithm.*

Withdrawal of this rejection and allowance of the claims is respectfully requested.

Applicant notes that the due date for this brief, being Saturday, May 12, 2005. Since this "due date falls on [a] Saturday... within the District of Columbia, the action may be taken, or the fee paid, on the next succeeding business day which is not a Saturday, Sunday, or a Federal holiday." 37 C.F.R. § 1.7. Accordingly, this filing is timely as filed on May 14, 2005, and no extension fee is due. However, if any fee is required or any overpayment made, the Commissioner is hereby authorized to charge the fee or credit the overpayment to Deposit Account # 18-0013.

Dated: May 14, 2007

Respectfully submitted,

By 40,290

Ronald P. Kananen
Registration No.: 24,104
Christopher M. Tobin
Registration No.: 40,290
RADER, FISHMAN & GRAUER PLLC
Correspondence Customer Number: 23353
(202) 955-3750
Attorney for Applicant